PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-197058
(43)Date of publication of application : 19.07.2001

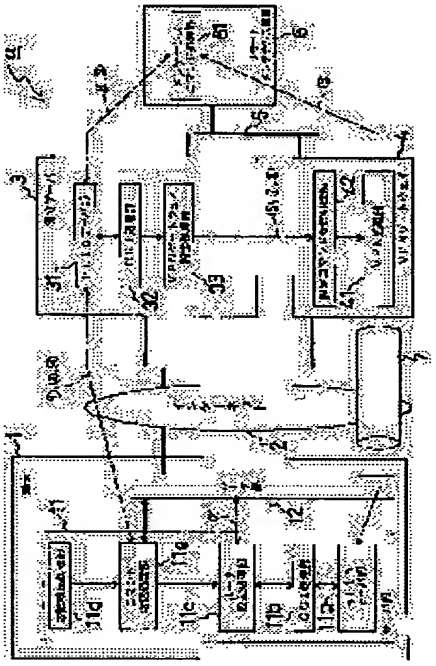
(51)Int.Cl. H04L 12/24
H04L 12/26
H04L 12/56

(21)Application number : 2000-000496
(22)Date of filing : 05.01.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NAKAHAMA KIYOSHI
YAMADA KEISHIN

(54) METHOD FOR SHARING AUTHENTICATION KEY BETWEEN TERMINAL AND MAINTENANCE SERVER AND METHOD FOR TERMINAL REMOTE MAINTENANCE IMPLEMENTATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a terminal-maintenance server authentication key sharing method and a terminal remote maintenance implementing method which can remotely maintain a terminal by IPsec with high security without any operator's operation on the terminal side.
SOLUTION: After a terminal 1 is authenticated accompanying specific sharing authentication information as a fault of the terminal 1 is detected, a fault code and the global IP address of the terminal 1 are sent to the maintenance server 3, the setting of an authentication key of IPsec and the initiator setting of IPsec are written to a VPN gateway 4 controlled with commands from the maintenance server 3, and then necessary remote maintenance is carried out for a server part 11 and a router part 12 of the terminal 1 through a VPN tunnel set between the terminal 1 and maintenance server 3 (VPN gateway 4).



LEGAL STATUS

[Date of request for examination] 27.11.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision

of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－197058
（P2001－197058A）
(43)公開日　平成13年７月19日(2001.7.19)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　12/24		Ｈ０４Ｌ　11/08		５Ｋ０３０
12/26		11/20	１０２Ｚ	
12/56				

審査請求　未請求　請求項の数15　ＯＬ　（全 19 頁）

(21)出願番号　特願2000－496(P2000－496)

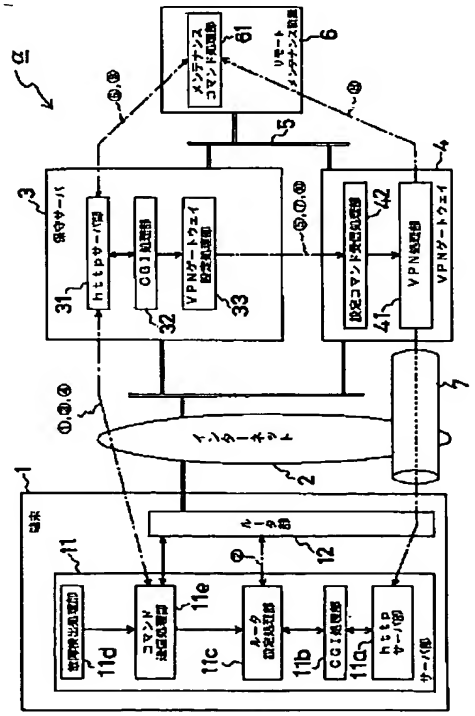
(22)出願日　平成12年１月５日(2000.1.5)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　中濱　清志
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　山田　敬信
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100071113
弁理士　菅　隆彦

Ｆターム(参考)　5K030 GA15 HD03 JA10 JT02 LD19 MA06 MB01

(54)【発明の名称】　端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法

(57)【要約】
【課題】ＩＰｓｅｃによる端末のリモートメンテナンスを、端末側における人間の操作なしにハイセキュリティに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法の提供。
【解決手段】端末１における故障検出に伴い、所定の共有認証情報に基づいて端末１の認証を行った後に、当該端末１の故障に係る故障コード及びグローバルＩＰアドレスを保守サーバ３へ送信すると共に、ＩＰｓｅｃの認証鍵の設定及びＩＰｓｅｃのイニシエータ設定を、保守サーバ３からコマンド制御されるＶＰＮゲートウェイ４に書き込み、これにより、端末１と保守サーバ３（ＶＰＮゲートウェイ４）との間に設定されるＶＰＮトンネル７を通じ、端末１のサーバ部１１及びルータ部１２に対し所要のリモートメンテナンスを実施する特徴。



1

【特許請求の範囲】

【請求項１】インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、ＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃの認証鍵を共有するに当り、

前記端末の設置時に、当該端末と前記保守サーバとで事前に共有される第１の共有認証情報に基づいて前記保守サーバ内で前記端末の認証を行い、この認証が成功した場合に、当該保守サーバ内で前記ＩＰｓｅｃの認証鍵及び第２の共有認証情報をランダムに生成すると共に、これら生成した認証鍵及び第２の共有認証情報を、公開鍵暗号方式を用いて前記端末へ受け渡す設置通知処理と、

該設置通知処理の完了に伴い、前記保守サーバから前記端末へ受け渡された前記認証鍵の設定を、当該端末のルータ部に書き込む端末ＶＰＮ鍵設定処理と、を実行する、

ことを特徴とする端末－保守サーバ間認証鍵共有方法。

【請求項２】前記設置通知処理は、

前記保守サーバ内での前記端末の認証に先立ち、

ユニークな端末ＩＤにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記第１の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、

前記保守サーバ内での前記端末の認証に際し、

前記端末から受信した前記原文に対し前記保守サーバ内の前記第１の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、

前記端末への前記認証鍵及び第２の共有認証情報の受渡しに先立ち、

前記端末内で生成した前記公開鍵暗号方式の公開鍵を前記保守サーバへ送信する処理と、

前記端末への前記認証鍵及び第２の共有認証情報の受渡しに際し、

前記端末から受信した前記公開鍵を用いて当該認証鍵及び第２の共有認証情報を暗号化し、これら暗号化後の認証鍵及び第２の共有認証情報を前記端末へ送信する処理と、

前記保守サーバから受信した当該暗号化後の認証鍵及び第２の共有認証情報を、前記端末内で前記公開鍵と共に生成した前記公開鍵暗号方式の秘密鍵を用いて復号化する処理と、を含む、

ことを特徴とする請求項１に記載の端末－保守サーバ間認証鍵共有方法。

【請求項３】前記端末ＶＰＮ鍵設定処理は、

前記認証鍵の設定の前記端末のルータ部への書込みに際し、前記保守サーバからコマンド制御されるＶＰＮゲートウェイを前記ＩＰｓｅｃの対象ホストとする処理を含む、

ことを特徴とする請求項１又は２に記載の端末－保守サーバ間認証鍵共有方法。

2

【請求項４】インターネットに端末型ダイヤルアップ接続された複数の端末を、ＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃにより、単一の保守サーバからリモートメンテナンスするに当り、

前記端末における故障の検出時に、当該端末と前記保守サーバとで事前に共有される所定の共有認証情報に基づいて、前記保守サーバ内で前記端末の認証を行うと共に、当該端末の故障に係る故障コードを前記保守サーバへ送信する故障通知処理と、

該故障通知処理の完了に伴い、前記所定の共有認証情報に基づいて、前記保守サーバにおいて前記端末の認証を行うと共に、前記端末型ダイヤルアップ接続に伴って前記端末のルータ部に設定されたグローバルＩＰアドレスを前記保守サーバへ送信するリモートメンテナンス要求処理と、

該リモートメンテナンス要求処理の完了に伴い、前記端末と前記保守サーバとで事前に共有される前記ＩＰｓｅｃの認証鍵の設定、及び前記グローバルＩＰアドレスにより特定される前記ＩＰｓｅｃのイニシエータ設定とを、前記保守サーバからコマンド制御されるＶＰＮゲートウェイに書き込むＶＰＮゲートウェイ設定処理と、

該ＶＰＮゲートウェイ設定処理の完了に伴い、前記保守サーバからのコマンド制御に応じて、前記端末と前記保守サーバとの間に所要の前記ＶＰＮセッションを設定するＶＰＮセッション開始指示処理と、

該ＶＰＮセッション開始指示の完了に伴い、前記故障コードの種別に応じた復旧指示コマンドの外部入力を受け付け、当該復旧指示コマンドの入力と共に、前記端末及び該端末のルータ部に対し所要の前記リモートメンテナンスを実施するリモートメンテナンス処理と、を実行する、

ことを特徴とする端末リモートメンテナンス実施方法。

【請求項５】前記故障通知処理は、

前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末ＩＤにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、

前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、

前記端末から受信した前記故障コードを前記保守サーバ内に保持する処理と、を含む、

ことを特徴とする請求項４に記載の端末リモートメンテナンス実施方法。

【請求項６】前記リモートメンテナンス要求処理は、

前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末ＩＤにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、

前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、

前記端末から受信した前記グローバルＩＰアドレスを前記保守サーバ内に保持する処理と、を含む、

ことを特徴とする請求項４又は５に記載の端末リモートメンテナンス実施方法。

【請求項７】前記ＶＰＮゲートウェイ設定処理は、

前記ＩＰｓｅｃの認証鍵の設定及び同ＩＰｓｅｃのイニシエータ設定の書込みに際し、前記端末のルータ部を前記ＩＰｓｅｃの対象ホストとする処理を含む、

ことを特徴とする請求項４、５又は６に記載の端末リモートメンテナンス実施方法。

【請求項８】前記ＶＰＮセッション開始指示処理は、

前記ＶＰＮセッションの設定に際し、前記ＶＰＮゲートウェイと前記端末のルータ部との間に前記ＩＰｓｅｃを確立する処理を含む、

ことを特徴とする請求項４、５、６又は７に記載の端末リモートメンテナンス実施方法。

【請求項９】前記リモートメンテナンス処理は、

前記リモートメンテナンスの実施に際し、前記復旧指示コマンドの入力を前記ＶＰＮゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記端末及び該端末のルータ部へ送信する処理を含む、

ことを特徴とする請求項４、５、６、７又は８に記載の端末リモートメンテナンス実施方法。

【請求項１０】前記ＶＰＮゲートウェイ設定処理と、前記ＶＰＮセッション開始指示処理の実行前は、

それら処理間に、さらに前記リモートメンテナンスの開始指示に係る開始指示コマンドの外部入力を受け付け、当該開始指示コマンドの入力と共に、前記保守サーバに対し前記ＶＰＮセッションの設定開始に係る指示を与えるリモートメンテナンス開始指示処理を実行する、

ことを特徴とする請求項４、５、６、７、８又は９に記載の端末リモートメンテナンス実施方法。

【請求項１１】前記リモートメンテナンス開始指示処理は、

前記リモートメンテナンスの開始指示に際し、前記開始指示コマンドの入力を前記ＶＰＮゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含む、

ことを特徴とする請求項１０に記載の端末リモートメンテナンス実施方法。

【請求項１２】前記リモートメンテナンス処理は、

その完了後に、さらに前記リモートメンテナンスの終了指示に係る終了指示コマンドの外部入力を受け付け、当該終了指示コマンドの入力と共に、前記保守サーバに対し前記ＶＰＮセッションの設定終了に係る指示を与えるリモートメンテナンス終了指示処理と、

該リモートメンテナンス終了指示処理の完了に伴い、前記ＶＰＮゲートウェイに書き込まれていた前記ＩＰｓｅｃの認証鍵の設定及び同ＩＰｓｅｃのイニシエータ設定を共に解除するＶＰＮセッション終了指示処理と、を実行する、

ことを特徴とする請求項４、５、６、７、８、９、１０又は１１に記載の端末リモートメンテナンス実施方法。

【請求項１３】前記リモートメンテナンス終了指示処理は、

前記リモートメンテナンスの終了指示に際し、前記終了指示コマンドの入力を前記ＶＰＮゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含む、

ことを特徴とする請求項１２に記載の端末リモートメンテナンス実施方法。

【請求項１４】前記ＶＰＮセッション終了指示処理は、

前記ＩＰｓｅｃの認証鍵の設定及び同ＩＰｓｅｃのイニシエータ設定の解除に際し、前記ＩＰｓｅｃの対象ホストとされていた前記端末のルータ部における各対応設定を解除する処理を含む、

ことを特徴とする請求項１２又は１３に記載の端末リモートメンテナンス実施方法。

【請求項１５】前記ＩＰｓｅｃの認証鍵、及び前記所定の共有認証情報は、それぞれ、

請求項１、２又は３に記載の端末－保守サーバ間認証鍵共有方法において前記端末と前記保守サーバとで共有される前記認証鍵、及び前記第２の共有認証情報を適用する、

ことを特徴とする請求項４、５、６、７、８、９、１０、１１、１２、１３又は１４に記載の端末リモートメンテナンス実施方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法に係わり、詳しくは、インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、ＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃの認証鍵を共有するための端末－保守サーバ間認証鍵共有方法、及びそれら複数の端末を、上記ＩＰｓｅｃにより実際に単一の保守

サーバからリモートメンテナンスするための端末リモートメンテナンス実施方法に関する。

【０００２】

【従来の技術】一般に、インターネットに端末型ダイヤルアップ接続された複数の端末を単一の保守サーバにより一元的に管理し、それら端末に故障が発生した際にメンテナンスを実施する場合、その第１の方法として、故障が発生した端末から保守サーバに対しインターネット経由で故障通知を自動的に送信し、これを確認した保守サーバの管理者が派遣修理を行うか、又は、当該管理者からの電話指示等により端末の所有者自身が修理を行う方法が採られており、所要のメンテナンスを保守サーバからリモートで実施することは行われていなかった。

【０００３】その主な理由としては、この第１の方法の場合、故障通知自体はダイヤルアップ接続により自動的に行われるものの、その故障通知後は、通常、端末内の無通信タイマにより短時間のうちに回線が切断されてしまい、リモートメンテナンスを実施しようとも、当該端末がインターネットにダイヤルアップ接続されているとは限らないためである。

【０００４】また、たとえ端末がダイヤルアップ接続されていたとしても、通常では、当該端末のＩＰアドレスを知ることができないため、保守サーバ側からの接続は不可能であり、仮に、そのＩＰアドレスを知ることができたとしても、インターネット経由でメンテナンスを実施するのは、ローカルネットワーク上のメンテナンスと比較してセキュリティ上の問題がある（例えば、ローカルメンテナンス用のツールをそのまま転用すると、各種秘密情報がインターネット上に漏洩するおそれがある）。

【０００５】こうした問題を解決するための第２の方法として、例えば、端末にリモートアクセスサーバ機能を具備させておき、故障通知後に、保守サーバの側から端末へ直接的に（インターネットを経由せずに）ダイヤルアップ接続を行い、さらに、コールバック等でセキュリティを確保した上で、所要のリモートメンテナンスを実施する方法が考えられる。

【０００６】しかし、この第２の方法では、故障通知を発した端末が保守サーバの設置場所から遠隔地にある場合、ダイヤルアップ接続にかかる通信コストが自ずと高くなり、加えて、端末にダイヤルアップ接続の着信を許容すると、当該端末及び該端末の内部ネットワークのセキュリティが著しく低下するなどの問題を生じる。

【０００７】このような問題に対処するため、第３の方法として、故障通知に伴い、端末の側からインターネット（プロバイダ）へダイヤルアップ接続し、ＯＳＩ参照モデルのネットワーク層においてアプリケーションに依存しない暗号通信を提供するＩＰｓｅｃ等のプロトコルにより、インターネットに接続された任意のリモートメンテナンス装置との間でＶＰＮセッションを設定し、当該ＶＰＮセッション上で、所要のリモートメンテナンスを実施する方法なども考えられる。

【０００８】このＩＰｓｅｃによるＶＰＮセッションの確立は、認証鍵（Presharedkey）の交換と、ＩＰｓｅｃプロトコルの１対１のグローバルＩＰアドレス通信とが可能であれば、技術的に何ら問題なく実現できる。

【０００９】ここで、端末型ダイヤルアップ接続によりＶＰＮセッションを確立し、所要のリモートメンテナンスを実施するための具体的手法を考察すれば、１）端末とＶＰＮゲートウェイとで認証鍵を共有，２）端末を端末型ダイヤルアップ接続によりインターネットプロバイダ経由でインターネットに接続，３）端末に割り当てられたグローバルＩＰアドレスを確認，４）回線切断前にＶＰＮゲートウェイの管理者にグローバルＩＰアドレスを連絡，５）双方で認証鍵交換の設定，６）双方でトンネルの設定，７）ＶＰＮによる通信／接続の確認，８）リモートメンテナンス処理を開始，９）リモートメンテナンスを運用（実施），１０）リモートメンテナンス処理を終了，１１）双方でトンネルの設定を解除，１２）双方で認証鍵交換の設定を解除，１３）接続を終了、といった手順が必要となる。

【００１０】

【発明が解決しようとする課題】ここで、端末のリモートメンテナンスを実施するには、上述した第３の方法を人間の操作を介在させずに行えることが理想である。

【００１１】しかしながら、上述もしたように、端末型ダイヤルアップ接続では、ＩＰアドレスは固定されないのが一般的なため、その都度、人間の操作でＩＰアドレス関連の設定を変更する必要があり、実際のメンテナンスの運用を無人で行うことは事実上不可能である。

【００１２】また、上述の認証鍵（Presharedkey）を２拠点のセキュリティゲートウェイ間で共有するには、それを紙面又は口頭で交換する必要があるなど、この場合にも人間の操作が介在し、ＩＰｓｅｃの運用が極めて煩雑なものになる。

【００１３】ここにおいて、本発明の解決すべき主要な目的は、次のとおりである。

【００１４】即ち、本発明の第１の目的は、ＩＰｓｅｃによる端末のリモートメンテナンスを、端末側における人間の操作なしにハイセキュリティに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法を提供せんとするものである。

【００１５】本発明の第２の目的は、ＩＰｓｅｃの確立を、人間の操作を介在させずに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法を提供せんとするものである。

【００１６】本発明の第３の目的は、２拠点のセキュリティゲートウェイにおける認証鍵の共有を、人間の操作を介在させずに行うことの可能な端末－保守サーバ間認証鍵共有方法及び端末リモートメンテナンス実施方法を

提供せんとするものである。

【００１７】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【００１８】

【課題を解決するための手段】本発明端末－保守サーバ間認証鍵共有方法においては、端末の設置時に、当該端末と保守サーバとで事前に共有される第１の共有認証情報に基づいて保守サーバ内で端末の認証を行った後に、当該保守サーバ内でＩＰｓｅｃの認証鍵及び第２の共有認証情報をランダムに生成し、これら認証鍵及び第２の共有認証情報を公開鍵暗号方式を用いて端末へ受け渡し、保守サーバから端末へ受け渡された認証鍵の設定を当該端末のルータ部に書き込む、という特徴を有する。

【００１９】本発明端末リモートメンテナンス実施方法においては、端末における故障検出に伴い、所定の共有認証情報に基づいて端末の認証を行った後に、当該端末の故障に係る故障コード及びグローバルＩＰアドレスを保守サーバへ送信すると共に、ＩＰｓｅｃの認証鍵の設定及びＩＰｓｅｃのイニシエータ設定を、保守サーバからコマンド制御されるＶＰＮゲートウェイに書き込み、これにより、端末と保守サーバとの間に設定されるＶＰＮセッション（ＶＰＮトンネル）を通じて、端末及び該端末のルータ部に対し所要のリモートメンテナンスを実施する、という特徴を有する。

【００２０】さらに具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する新規な特徴的構成手法を採用することにより、前記目的を達成するよう為される。

【００２１】即ち、本発明端末－保守サーバ間認証鍵共有方法の第１の特徴は、インターネットに端末型ダイヤルアップ接続された複数の端末と単一の保守サーバとの間で、ＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃの認証鍵を共有するに当り、前記端末の設置時に、当該端末と前記保守サーバとで事前に共有される第１の共有認証情報に基づいて前記保守サーバ内で前記端末の認証を行い、この認証が成功した場合に、当該保守サーバ内で前記ＩＰｓｅｃの認証鍵及び第２の共有認証情報をランダムに生成すると共に、これら生成した認証鍵及び第２の共有認証情報を、公開鍵暗号方式を用いて前記端末へ受け渡す設置通知処理と、該設置通知処理の完了に伴い、前記保守サーバから前記端末へ受け渡された前記認証鍵の設定を、当該端末のルータ部に書き込む端末ＶＰＮ鍵設定処理とを実行してなる、端末－保守サーバ間認証鍵共有方法の構成採用にある。

【００２２】本発明端末－保守サーバ間認証鍵共有方法の第２の特徴は、上記本発明端末－保守サーバ間認証鍵共有方法の第１の特徴における前記設置通知処理が、前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末ＩＤにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記第１の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記第１の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、前記端末への前記認証鍵及び第２の共有認証情報の受渡しに先立ち、前記端末内で生成した前記公開鍵暗号方式の公開鍵を前記保守サーバへ送信する処理と、前記端末への前記認証鍵及び第２の共有認証情報の受渡しに際し、前記端末から受信した前記公開鍵を用いて当該認証鍵及び第２の共有認証情報を暗号化し、これら暗号化後の認証鍵及び第２の共有認証情報を前記端末へ送信する処理と、前記保守サーバから受信した当該暗号化後の認証鍵及び第２の共有認証情報を、前記端末内で前記公開鍵と共に生成した前記公開鍵暗号方式の秘密鍵を用いて復号化する処理とを含んでなる、端末－保守サーバ間認証鍵共有方法の構成採用にある。

【００２３】本発明端末－保守サーバ間認証鍵共有方法の第３の特徴は、上記本発明端末－保守サーバ間認証鍵共有方法の第１又は第２の特徴における前記端末ＶＰＮ鍵設定処理が、前記認証鍵の設定の前記端末のルータ部への書込みに際し、前記保守サーバからコマンド制御されるＶＰＮゲートウェイを前記ＩＰｓｅｃの対象ホストとする処理を含んでなる、端末－保守サーバ間認証鍵共有方法の構成採用にある。

【００２４】また、本発明端末リモートメンテナンス実施方法の第１の特徴は、インターネットに端末型ダイヤルアップ接続された複数の端末を、ＯＳＩ参照モデルのネットワーク層においてＶＰＮセッションを実現するＩＰｓｅｃにより、単一の保守サーバからリモートメンテナンスするに当り、前記端末における故障の検出時に、当該端末と前記保守サーバとで事前に共有される所定の共有認証情報に基づいて、前記保守サーバ内で前記端末の認証を行うと共に、当該端末の故障に係る故障コードを前記保守サーバへ送信する故障通知処理と、該故障通知処理の完了に伴い、前記所定の共有認証情報に基づいて、前記保守サーバにおいて前記端末の認証を行うと共に、前記端末型ダイヤルアップ接続に伴って前記端末のルータ部に設定されたグローバルＩＰアドレスを前記保守サーバへ送信するリモートメンテナンス要求処理と、該リモートメンテナンス要求処理の完了に伴い、前記端末と前記保守サーバとで事前に共有される前記ＩＰｓｅｃの認証鍵の設定、及び前記グローバルＩＰアドレスにより特定される前記ＩＰｓｅｃのイニシエータ設定とを、前記保守サーバからコマンド制御されるＶＰＮゲートウェイに書き込むＶＰＮゲートウェイ設定処理と、該ＶＰＮゲートウェイ設定処理の完了に伴い、前記保守サ

ーバからのコマンド制御に応じて、前記端末と前記保守サーバとの間に所要の前記ＶＰＮセッションを設定するＶＰＮセッション開始指示処理と、該ＶＰＮセッション開始指示の完了に伴い、前記故障コードの種別に応じた復旧指示コマンドの外部入力を受け付け、当該復旧指示コマンドの入力と共に、前記端末及び該端末のルータ部に対し所要の前記リモートメンテナンスを実施するリモートメンテナンス処理とを実行してなる、端末リモートメンテナンス実施方法の構成採用にある。

【００２５】本発明端末リモートメンテナンス実施方法の第２の特徴は、上記本発明端末リモートメンテナンス実施方法の第１の特徴における前記故障通知処理が、前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末ＩＤにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、前記端末から受信した前記故障コードを前記保守サーバ内に保持する処理とを含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００２６】本発明端末リモートメンテナンス実施方法の第３の特徴は、上記本発明端末リモートメンテナンス実施方法の第１又は第２の特徴における前記リモートメンテナンス要求処理が、前記保守サーバ内での前記端末の認証に先立ち、ユニークな端末ＩＤにタイムスタンプを付加してなる原文と、この原文に対し前記端末内の前記所定の共有認証情報を用いて生成したメッセージ認証子とを前記保守サーバへ送信する処理と、前記保守サーバ内での前記端末の認証に際し、前記端末から受信した前記原文に対し前記保守サーバ内の前記所定の共有認証情報を用いて生成したメッセージ認証子が、同端末から受信した前記メッセージ認証子と一致するか否かを判別する処理と、前記端末から受信した前記グローバルＩＰアドレスを前記保守サーバ内に保持する処理とを含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００２７】本発明端末リモートメンテナンス実施方法の第４の特徴は、上記本発明端末リモートメンテナンス実施方法の第１、第２又は第３の特徴における前記ＶＰＮゲートウェイ設定処理が、前記ＩＰｓｅｃの認証鍵の設定及び同ＩＰｓｅｃのイニシエータ設定の書込みに際し、前記端末のルータ部を前記ＩＰｓｅｃの対象ホストとする処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００２８】さらに、本発明端末リモートメンテナンス実施方法の第５の特徴は、上記端末リモートメンテナンス実施方法の第１、第２、第３又は第４の特徴における前記ＶＰＮセッション開始指示処理が、前記ＶＰＮセッションの設定に際し、前記ＶＰＮゲートウェイと前記端末のルータ部との間に前記ＩＰｓｅｃを確立する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００２９】本発明端末リモートメンテナンス実施方法の第６の特徴は、上記端末リモートメンテナンス実施方法の第１、第２、第３、第４又は第５の特徴における前記リモートメンテナンス処理が、前記リモートメンテナンスの実施に際し、前記復旧指示コマンドの入力を前記ＶＰＮゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記端末及び該端末のルータ部へ送信する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３０】本発明端末リモートメンテナンス実施方法の第７の特徴は、上記端末リモートメンテナンス実施方法の第１、第２、第３、第４、第５又は第６の特徴における前記ＶＰＮゲートウェイ設定処理と、前記ＶＰＮセッション開始指示処理が、それら処理間に、さらに、前記リモートメンテナンスの開始指示に係る開始指示コマンドの外部入力を受け付け、当該開始指示コマンドの入力と共に、前記保守サーバに対し前記ＶＰＮセッションの設定開始に係る指示を与えるリモートメンテナンス開始指示処理を実行してなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３１】本発明端末リモートメンテナンス実施方法の第８の特徴は、上記端末リモートメンテナンス実施方法の第７の特徴における前記リモートメンテナンス開始指示処理が、前記リモートメンテナンスの開始指示に際し、前記開始指示コマンドの入力を前記ＶＰＮゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３２】本発明端末リモートメンテナンス実施方法の第９の特徴は、上記端末リモートメンテナンス実施方法の第１、第２、第３、第４、第５、第６、第７又は第８の特徴における前記リモートメンテナンス処理が、その完了後に、さらに、前記リモートメンテナンスの終了指示に係る終了指示コマンドの外部入力を受け付け、当該終了指示コマンドの入力と共に、前記保守サーバに対し前記ＶＰＮセッションの設定終了に係る指示を与えるリモートメンテナンス終了指示処理と、該リモートメンテナンス終了指示処理の完了に伴い、前記ＶＰＮゲートウェイに書き込まれていた前記ＩＰｓｅｃの認証鍵の設定及び同ＩＰｓｅｃのイニシエータ設定を共に解除するＶＰＮセッション終了指示処理とを実行してなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３３】本発明端末リモートメンテナンス実施方法の第１０の特徴は、上記端末リモートメンテナンス実施方法の第９の特徴における前記リモートメンテナンス終了指示処理が、前記リモートメンテナンスの終了指示に際し、前記終了指示コマンドの入力を前記ＶＰＮゲートウェイにローカルネットワーク接続された任意のリモートメンテナンス装置から受け付けて、これを前記保守サーバへ送信する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３４】本発明端末リモートメンテナンス実施方法の１１の特徴は、上記端末リモートメンテナンス実施方法の第９又は第１０の特徴における前記ＶＰＮセッション終了指示処理が、前記ＩＰｓｅｃの認証鍵の設定及び同ＩＰｓｅｃのイニシエータ設定の解除に際し、前記ＩＰｓｅｃの対象ホストとされていた前記端末のルータ部における各対応設定を解除する処理を含んでなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３５】本発明端末リモートメンテナンス実施方法の第１２の特徴は、上記端末リモートメンテナンス実施方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における前記ＩＰｓｅｃの認証鍵、及び前記所定の共有認証情報に、それぞれ、請求項１、２又は３に記載の端末ー保守サーバ間認証鍵共有方法において前記端末と前記保守サーバとで共有される前記認証鍵、及び前記第２の共有認証情報を適用してなる、端末リモートメンテナンス実施方法の構成採用にある。

【００３６】

【発明の実施の形態】以下、本発明の実施の形態を、添付図面を参照しつつ、まず、本発明の適用を受ける適用システムの構成例につき説明し、次いで、当該適用システムにおいて実施される方法例につき説明する。

【００３７】（適用システム構成例）図１は、本発明の適用システムであるリモートメンテナンスシステムの構成を示す図である。

【００３８】同図に示すように、このリモートメンテナンスシステムαは、４つのノード、即ち、リモートメンテナンスの対象となる端末１と、この端末１にインターネット２を経由して接続される保守サーバ３と、この保守サーバ３からコマンド制御されるＶＰＮゲートウェイ４と、このＶＰＮゲートウェイ４にＬＡＮ等のローカルネットワーク５で接続されたリモートメンテナンス装置６とを有して構成される。また、端末１と保守サーバ３との間には、ＶＰＮゲートウェイ４を経由してＶＰＮトンネル７が設定される。

【００３９】端末１は、本発明における故障検出機能及び復旧機能を実現するサーバ部１１と、ＩＰｓｅｃを含んだＩＰルータ処理を制御するルータ部１２とを有して構成され、このうちのサーバ部１１は、さらに、ｈｔｔｐサーバ処理を行うｈｔｔｐサーバ部１１ａと、このｈｔｔｐサーバ部１１ａからコールされて内部処理を行うＣＧＩ処理部１１ｂと、ルータ部１２への制御コマンドを発行するルータ設定処理部１１ｃと、端末１及びルータ部１２の故障を検出する故障検出処理部１１ｄと、保守サーバ３に所要のコマンドを送信するコマンド送信処理部１１ｅとを有して構成される。

【００４０】保守サーバ３は、端末１から送信されるｈｔｔｐコマンドを受信するｈｔｔｐサーバ部３１と、このｈｔｔｐサーバ部３１からコールされて内部処理を行うＣＧＩ処理部３２と、ＶＰＮゲートウェイ４へｔｅｌｎｅｔコマンドを発行するＶＰＮゲートウェイ設定処理部３３とを有して構成される。

【００４１】ＶＰＮゲートウェイ４は、端末１のルータ部１２との間でＶＰＮセッションを行うＶＰＮ処理部４１と、保守サーバ３のＶＰＮゲートウェイ設定処理部３３から送信されるｔｅｌｎｅｔコマンドを受信する設定コマンド受信処理部４２とを有して構成される。

【００４２】リモートメンテナンス装置６は、端末１のサーバ部１１に対し、ｈｔｔｐコマンド等によりコマンドを送信するメンテナンスコマンド処理部６１を有して構成される。

【００４３】なお、以上のリモートメンテナンスシステムαは、その説明からも明らかなように、各ノード間の通信プロトコルとして、ｈｔｔｐやｔｅｌｎｅｔを適用することを前提としたものだが、各処理部間の通信が円滑に行えれば、その通信プロトコルの種別は特に問うものではない。但し、本発明では、インターネット間の通信を前提としているため、ＴＣＰ／ＩＰ上の通信プロトコルであることは必須である（汎用性を考慮すると、ｈｔｔｐからＣＧＩを起動する形態であることが望ましい）。

【００４４】

【外１】

13　　14

ここで、図示の①～⑩は、本発明において実行される各処理の通信データ（コマンド送信及び受信）のルートを示しており、それぞれ、①は「設置通知処理」の、②は「端末ＶＰＮ鍵設定処理」の、③は「故障通知処理」の、④は「リモートメンテナンス要求処理」の、⑤は「ＶＰＮゲートウェイ設定処理」の、⑥は「リモートメンテナンス開始指示処理」の、⑦は「ＶＰＮセッション開始指示処理」の、⑧は「リモートメンテナンス処理」の、⑨は「リモートメンテナンス終了指示処理」、⑩は「ＶＰＮセッション終了指示処理」の通信データのルートである。

【００４５】このうち、　及び　の処理は、本発明における端末－保守サーバ間認証鍵共有方法を実現するための処理であり、これらの処理は、端末１の設置時に一度だけ実行される。

【００４６】

【外２】

また、残る③～⑩の処理は、本発明における端末リモートメンテナンス実施方法を実現するための処理であり、これら一連の処理は、リモートメンテナンスの実施が要求されることに実行される。このうち、リモートメンテナンス装置６から起動される⑥，⑧及び⑨の処理については、人間の操作が必要とされるが、その他の端末１側からの処理は、当該端末１における故障発生の検出を受け、各処理が連携しながら自動的に起動される。

【００４７】なお、本発明の実施に際しては、以下に示す前提条件が必要とされる。

【００４８】（１）（複数の）端末１が、その出荷時において個々にユニークな端末ＩＤを持つこと。

【００４９】（２）端末１と保守サーバ３が、本発明にいう第１の共有認証情報を事前に共有していること（以下、第１の共有認証情報を、「Secret(id)」とも表記する。「id」は、端末ＩＤと同一の値であり、従って、Secret(id)は、端末ＩＤごとにユニークな共有秘密情報である）。なお、Secret(id)は、端末１の出荷時に、当該端末１内のＲＯＭ等に埋め込み、保守サーバ３と共有することで対応する（当該Secret(id)は、保守サーバ３がリモートメンテナンスを行う全ての端末１で共通であってもよい）。

【００５０】（３）端末１のルータ部１２が、ＩＰｓｅｃ等のＩＰレベルのＶＰＮ機能を持ち、また、ＶＰＮセッションについて、セッション待受け側の設定を事前に行っておくこと（ＩＰｓｅｃの場合は、当該ルータ部１２をレスポンダとして設定する）。なお、認証鍵（以下、「Presharedkey」とも表記する）にはダミーデータを設定しておくこと。

【００５１】（４）ＶＰＮゲートウェイ４が、端末１のルータ部１２と通信互換性のあるＶＰＮ機能を持つこと。

【００５２】（５）端末１のルータ部１２が、保守サーバ３の公開されたグローバルＩＰアドレス、又はこれと等価のインターネットホスト名を、　の設置通知処理の時点までに事前に知っていること。また、インターネットへの接続手段として、端末型ダイヤルアップ接続を適用することとし、その設定が既に完了していること。

【００５３】（６）端末１のサーバ部１１におけるルータ設定処理部１１ｃからルータ部１２への各種通信設定が、リモートコンソール（以下、「ｔｅｌｎｅｔ」という）又はプロセス間通信で行えること。

【００５４】（７）保守サーバ３のＶＰＮゲートウェイ設定処理部３３からＶＰＮゲートウェイ４の設定コマンド受信処理部４２への各種通信設定が、ｔｅｌｎｅｔで行えること。

【００５５】（８）　の設置通知処理、　の故障通知処理、及び　のリモートメンテナンス要求処理におけるメッセージ認証子（以下、「ＭＡＣ」とも表記する）の計算アルゴリズムが、端末１と保守サーバ３とで共通であること。（以上、実施前提条件）

【００５６】（方法例）続いて、上述したリモートメンテナンスシステムαに適用される方法例について説明する。なお、本発明は、「端末－保守サーバ間認証鍵共有方法」と「端末リモートメンテナンス実施方法」とを包含するものであるが、両者は互いに密接な関係を有するため、本方法例においては、これらを特に区別することなく説明するものとする。

【００５７】＜　設置通知処理＞本設置通知処理は、端末１が設置されたことをリモートメンテナンスに先立って保守サーバ３へ通知し、その保守３サーバから、本発明にいう第２の共有認証情報を受け取ることを目的とする（以下、第２の認証情報を、「Secret２(id)」とも表記する。「id」は、端末ＩＤと同一の値であり、従って、Secret２(id)は、端末ＩＤごとにユニークな共有秘密情報である）。なお、ここで、Secret(id)の代わりにSecret２(id)を用いるのは、端末１の全てに共通している可能性があるSecret(id)よりも、このSecret２(id)を用いた方が、セキュリティが強化されるためである。以下、図面により、本設置通知処理の詳細を説明する。

【００５８】図２は、本発明の方法例に係る設置通知処理を説明するためのフローチャートである。

【００５９】同図に示すように、本設置通知処理は、端末１の設置終了後（ＳＴ１）、インターネット２への接続設定が完了した時点で（ＳＴ２）、当該端末１の管理者（所有者）の操作により、サーバ部１１において一度だけ実行される。

【００６０】即ち、サーバ部１１は、そのコマンド送信処理部１１ｅにおいて、まず、公開鍵暗号化方式のアルゴリズム（ＲＳＡ等）により、秘密鍵及び公開鍵を生成すると共に（ＳＴ３）、端末ＩＤに現在のタイムスタンプを付加してなる原文を作成し（ＳＴ４）、さらに、この原文に対し、端末１内に事前に設定されたSecret(id)を用いてメッセージ認証子（ＭＡＣ）を生成する（ＳＴ５）。なお、このメッセージ認証子の生成に際しては、ＩＳＯ９７９７－１及びＩＳＯ９７９７－２に準拠することが望ましい（以下、メッセージ認証子の生成について同じ）。

【００６１】そして、コマンド送信処理部１１ｅは、「設置通知を示すコード」，「端末ＩＤ」，「原文」，「ＭＡＣ」，及び「公開鍵」をパラメータとしたｈｔｔｐコマンドを、非ＩＰｓｅｃセッションにより、保守サーバ３のｈｔｔｐサーバ部３１に向けて送信する（ＳＴ６）。

【００６２】保守サーバ３のｈｔｔｐサーバ部３１では、端末１から送信された上記コマンドを受信し（ＳＴ７）、その受信に係るコマンド名及びパラメータをＣＧＩ処理部３２へ受け渡す。

【００６３】ＣＧＩ処理部３２は、上記パラメータ中の原文に対し、保守サーバ３内に事前に設定されたSecret(id)を用いてメッセージ認証子（ＭＡＣ）を生成し（端末１におけるそれと同様の演算）、これが上記パラメータ中のＭＡＣと一致することを確認して、端末１の認証を行う（ＳＴ８）。

【００６４】そして、ＣＧＩ処理部３２は、ＩＰｓｅｃの認証鍵であるPresharedkeyとSecret２(id)とをランダムに生成し（ＳＴ９，ＳＴ１０）、これらを、上記パラメータ中の端末ＩＤに対応したデータとして自身に保持すると共に、同パラメータ中の暗号鍵で暗号化する（ＳＴ１１）。

【００６５】次に、保守サーバ３のｈｔｔｐサーバ部３１は、上記ＣＧＩ処理部３２から、端末１の認証に関する「ステータス（正常又はエラーステータス）」，「暗号化後のPresharedkey」，及び「暗号化後のSecret２(id)」を取得し、これらをパラメータとしたｈｔｔｐレスポンスを、非ＩＰｓｅｃセッションにより、端末１のサーバ部１１におけるコマンド送信処理部１１ｅに向け送信する（ＳＴ１２）。

【００６６】そして、端末１のサーバ部１１におけるコマンド送信処理部１１ｅは、保守サーバ３から送信された上記レスポンスを受信し（ＳＴ１３）、これに含まれるパラメータ中の暗号化後のPresharedkey及び同Secret２(id)を、それぞれ先に生成しておいた秘密鍵で復号化して自身に保持し（ＳＴ１４，ＳＴ１５）、処理を　の端末ＶＰＮ鍵設定処理へと受け渡す（図示の記号「Ａ」により連続）。

【００６７】なお、端末１の後処理として、これ以降に用いられることのないSecret(id)を消去すれば、よりセキュリティが強まるが、これは必須ではない。

【００６８】＜　端末ＶＰＮ鍵設定処理＞本端末ＶＰＮ鍵設定処理は、上述の設置通知処理の完了後、端末１のルータ部１２に対しPresharedkeyを設定することを目的とする。以下、図面により、本端末ＶＰＮ鍵設定処理の詳細を説明する。

【００６９】図３は、本発明の方法例に係る端末ＶＰＮ鍵設定処理を説明するためのフローチャートである。

【００７０】同図に示すように、本端末ＶＰＮ鍵設定処理は、上述の設置通知処理の完了を契機（Ａ）に開始される。即ち、端末１のサーバ部１１におけるルータ設定処理部１１ｃは、Presharedkeyの取得に伴い（ＳＴ１６）、まず、ＶＰＮゲートウェイ４をＩＰｓｅｃの対象ホストとした「Presharedkeyの設定（ルータ部１２のｔｅｌｎｅｔコマンドの実装形態により異なる）」をパラメータとしたｔｅｌｎｅｔコマンドを、ローカルネットワークセッションにより、同端末１のルータ部１２に向けて送信する（ＳＴ１７）。

【００７１】ルータ部１２は、サーバ部１１から送信された上記コマンドを受信し（ＳＴ１８）、その受信に係るコマンド中のパラメータであるPresharedkeyの設定を自身に書き込み（ＳＴ１９）、さらに、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとしたｔｅｌｎｅｔレスポンスを、ローカルネットワークセッションにより、同端末１のサーバ部１１におけるルータ設定処理部１１ｃに向けて送信し（ＳＴ２０）、所要のＶＰＮ設定を完了する。

【００７２】そして、端末１のサーバ部１１におけるルータ設定処理部１１ｃは、ルータ部１２から送信された上記レスポンスを受信し（ＳＴ２１）、以上により、所要の端末１の設置に係る全ての処理（　の設置通知処理、及び　の端末ＶＰＮ鍵設定処理）を完了する。

【００７３】＜　故障通知処理＞本故障通知処理は、端末１のサーバ部１１及びルータ部１２に故障が発生したことを随時に検出し、その状態を保守サーバ３に通知することを目的とする。以下、図面により、本故障通知処理の詳細を説明する。

【００７４】図４は、本発明の方法例に係る故障通知処理を説明するためのフローチャートである。

【００７５】同図に示すように、本故障通知処理は、端末１のサーバ部１１における故障検出処理部１１ｄが、同端末１のサーバ部１１及びルータ部１２に故障が発生

したことを検出した時点で開始される（ＳＴ３１）。即ち、この故障検出処理部１１ｄは、サーバ部１１及びルータ部１２における故障の発生及び復旧の状態を常時監視し、何らかの故障が発生した時点で、本故障通知処理を起動する。

【００７６】端末１に故障が検出されると、同端末１のサーバ部１１におけるコマンド送信処理部１１ｅは、まず、端末ＩＤに現在のタイムスタンプを付加してなる原文を作成し（ＳＴ３２）、さらに、この原文に対し、端末１内に新たに設定されたSecret２(id)を用いてメッセージ認証子（ＭＡＣ）を生成する（ＳＴ３３）。

【００７７】そして、コマンド送信処理部１１ｅは、「故障通知を示すコード」，「端末ＩＤ」，「原文」，「ＭＡＣ」，及び「故障コード」をパラメータとしたｈｔｔｐコマンドを、非ＩＰｓｅｃセッションにより、保守サーバ３のｈｔｔｐサーバ部３１に向けて送信する（ＳＴ３４）。

【００７８】保守サーバ３のｈｔｔｐサーバ部３１では、端末１から送信された上記コマンドを受信し（ＳＴ３５）、その受信に係るコマンド名及びパラメータをＣＧＩ処理部３２へ受け渡す。

【００７９】ＣＧＩ処理部３２は、上記パラメータ中の原文に対し、保守サーバ３内に新たに設定されたSecret２(id)を用いてメッセージ認証子（ＭＡＣ）を生成し（端末１におけるそれと同様の演算）、これが上記パラメータ中のＭＡＣと一致することを確認して、端末１の認証を行い（ＳＴ３６）、さらに、上記パラメータ中の故障コードを、同パラメータ中の端末ＩＤに対応したデータとして自身に保持する（ＳＴ３７）。

【００８０】次に、保守サーバ３のｈｔｔｐサーバ部３１は、上記ＣＧＩ処理部３２から、端末１の認証に関する「ステータス（正常又はエラーステータス）」を取得し、当該ステータスをパラメータとしたｈｔｔｐレスポンスを、非ＩＰｓｅｃセッションにより、端末１のサーバ部１１におけるコマンド送信処理部１１ｅに向けて送信する（ＳＴ３８）。

【００８１】そして、端末１のサーバ部１１におけるコマンド送信処理部１１ｅは、保守サーバ３から送信された上記レスポンスを受信し（ＳＴ３９）、以上により、この故障通知処理を完了して、処理を　のリモートメンテナンス要求処理へと受け渡す（図示の記号「Ｂ」により連続）。

【００８２】なお、本故障通知処理において、端末ＩＤに対応したデータとして保持した故障コードは、端末１における故障状態の確認のため、リモートメンテナンス装置６からｈｔｔｐアクセス等により参照できることが望ましい。

【００８３】＜　リモートメンテナンス要求処理＞本リモートメンテナンス要求処理は、上述の故障通知処理と連動して、ＩＰｓｅｃによるリモートメンテナンスの実施を保守サーバ３に要求することを目的とする。但し、故障通知処理と連動したリモートメンテナンスが速やかに行われない場合は、インターネット２との接続が切断されて、確立したＶＰＮトンネル７が消失する可能性があるため、端末１の管理者が、当該リモートメンテナンス要求処理を手動操作で立ち上げることも併せて許容する。以下、図面により、本リモートメンテナンス要求処理の詳細を説明する。

【００８４】図５は、本発明の方法例に係るリモートメンテナンス要求処理及びＶＰＮゲートウェイ設定処理を説明するためのフローチャートである。

【００８５】同図に示すように、本リモートメンテナンス要求処理は、上述の故障通知処理の完了を契機（Ｂ）に、又は、端末１の管理者のボタン操作等による当該端末１へのアクション（ＳＴ４０）に応じて開始される。即ち、端末１のサーバ部１１におけるコマンド送信処理部１１ｅは、まず、端末１がインターネット２に接続されているか否かを判別し（ＳＴ４１）、それが未だ接続されていない場合には（ＳＴ４１；Ｎ）、インターネット２に接続した後に（ＳＴ４２）、既に接続されている場合には（ＳＴ４１；Ｙ）、直ちに、端末ＩＤに現在のタイムスタンプを付加してなる原文を作成し（ＳＴ４３）、さらに、この原文に対し、端末１内に設定されたSecret２(id)を用いてメッセージ認証子（ＭＡＣ）を生成する（ＳＴ４４）。

【００８６】そして、コマンド送信処理部１１ｅは、端末１のルータ部１２から、ダイヤルアップ接続時にインターネットプロバイダからＩＰＣＰで割り当てられた、当該ルータ部１２のグローバルＩＰアドレスを取得し（ＳＴ４５）、さらに、「リモートメンテナンス要求を示すコード」，「端末ＩＤ」，「原文」，「ＭＡＣ」，及び「グローバルＩＰアドレス」をパラメータとしたｈｔｔｐコマンドを、非ＩＰｓｅｃセッションにより、保守サーバ３のｈｔｔｐサーバ部３１に向けて送信する（ＳＴ４６）。

【００８７】保守サーバ３のｈｔｔｐサーバ部３１では、端末１から送信された上記コマンドを受信し（ＳＴ４７）、その受信に係るコマンド名及びパラメータをＣＧＩ処理部３２へ受け渡す。

【００８８】ＣＧＩ処理部３２は、上記パラメータ中の原文に対し、保守サーバ３内に設定されたSecret２(id)を用いてメッセージ認証子（ＭＡＣ）を生成し（端末１におけるそれと同様の演算）、これが上記パラメータ中のＭＡＣと一致することを確認して、端末１の認証を行い（ＳＴ４８）、さらに、上記パラメータ中のグローバルＩＰアドレス（以下、「ルータＩＰアドレス」という）を、同パラメータ中の端末ＩＤに対応したデータとして自身に保持する（ＳＴ４９）。

【００８９】次に、保守サーバ３のｈｔｔｐサーバ部３１は、上記ＣＧＩ処理部３２から、端末１の認証に関す

る「ステータス（正常又はエラーステータス）」を取得し、当該ステータスをパラメータとしたｈｔｔｐレスポンスを、非ＩＰｓｅｃセッションにより、端末１のサーバ部１１におけるコマンド送信処理部１１ｅに向けて送信する（ＳＴ５０）。

【００９０】そして、端末１のサーバ部１１におけるコマンド送信処理部１１ｅは、保守サーバ３から送信された上記レスポンスを受信し（ＳＴ５１）、以上により、このリモートメンテナンス要求処理を完了して、処理をのＶＰＮゲートウェイ設定処理へと受け渡す。

【００９１】＜　ＶＰＮゲートウェイ設定処理＞本ＶＰＮゲートウェイ設定処理は、上述のリモートメンテナンス要求処理と連動して、保守サーバ３で受信されたルータＩＰアドレスをもとに、ＶＰＮゲートウェイ４に対し、Presharedkeyの設定及びＩＰｓｅｃイニシエータ設定の書込みを行うことを目的とする。以下、前述の図５により、本ＶＰＮゲートウェイ設定処理の詳細を説明する。

【００９２】同図に示すように、本ＶＰＮゲートウェイ設定処理は、上述のリモートメンテナンス要求処理における正常終了レスポンスの送信を契機（ＳＴ５０のステップ）に開始される。即ち、保守サーバ３のＶＰＮゲートウェイ設定処理部３３は、まず、ＣＧＩ処理部３２から、ＩＰｓｅｃの認証鍵であるPresharedkeyとルータＩＰアドレスとを取得して（ＳＴ５２，ＳＴ５３）、端末１のルータ部１２をそれぞれＩＰｓｅｃの対象ホストとした「Presharedkeyの設定（ＶＰＮゲートウェイ４のｔｅｌｎｅｔコマンドの実装形態により異なる）」，及び「ＩＰｓｅｃイニシエータ設定（ＶＰＮゲートウェイ４のｔｅｌｎｅｔコマンドの実装形態により異なる）」をパラメータとしたｔｅｌｎｅｔコマンドを生成し（ＳＴ５４）、当該コマンドを、ローカルネットワークセッションにより、ＶＰＮゲートウェイ４に向けて送信する（ＳＴ５５）。

【００９３】ＶＰＮゲートウェイ４は、その設定コマンド受信処理部４２において、保守サーバ３から送信された上記コマンドを受信し（ＳＴ５６）、その受信に係るコマンド中のパラメータであるPresharedkeyの設定とＩＰｓｅｃイニシエータの設定とを自身に書き込み（ＳＴ５７）、さらに、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとしたｔｅｌｎｅｔレスポンスを、ローカルネットワークセッションにより、保守サーバ３のＶＰＮゲートウェイ設定処理部３３に向けて送信し（ＳＴ５８）、所要のＶＰＮ設定を完了する。

【００９４】そして、保守サーバ３のＶＰＮゲートウェイ設定処理部３３は、ＶＰＮゲートウェイ４から送信された上記レスポンスを受信し（ＳＴ５９）、以上により、本ＶＰＮゲートウェイ設定処理を完了する。

【００９５】なお、以上のＶＰＮ設定が完了した段階で、その状態がリモートメンテナンス装置６から確認できることが望ましい。その理由は、ＶＰＮ設定が完了したことを確認した上で、以降に続く　のリモートメンテナンス開始指示処理を実行できた方が、リモートメンテナンスの実施者の作業効率が良いからである（リモートメンテナンス開始指示処理の成功する確率が高い）。

【００９６】＜　リモートメンテナンス開始指示処理＞本リモートメンテナンス開始指示処理は、リモートメンテナンス装置６を使用して、実際にリモートメンテナンスを開始することを保守サーバ３に伝えることを目的とする。以下、図面により、本リモートメンテナンス開始指示処理の詳細を説明する。

【００９７】図６は、本発明の方法例に係るリモートメンテナンス開始指示処理を説明するためのフローチャートである。

【００９８】同図に示すように、本リモートメンテナンス開始指示処理は、リモートメンテナンスの実施者の手動操作により開始される。即ち、リモートメンテナンス装置６のメンテナンスコマンド処理部６１は、「リモートメンテナンス開始を示すコード」をパラメータとしたｈｔｔｐコマンドを、ローカルネットワークセッションにより、保守サーバ３のｈｔｔｐサーバ部３１に向け送信する（ＳＴ６０）。

【００９９】保守サーバ３のｈｔｔｐサーバ部３１では、リモートメンテナンス装置６から送信された上記コマンドを受信し（ＳＴ６１）、以下、処理を　のＶＰＮセッション開始指示処理へと受け渡す（図示の記号「Ｃ」により連続）。

【０１００】なお、本リモートメンテナンス開始指示処理は、実際には、以降に続くＶＰＮセッション開始指示処理が完了するまで起動状態を維持する。その詳細については、以下のＶＰＮセッション開始指示処理で併せて説明する（図示の記号「Ｄ」により連続）。

【０１０１】＜　ＶＰＮセッション開始指示処理＞本ＶＰＮセッション開始指示処理は、上述のリモートメンテナンス開始指示処理の内部処理として機能し、リモートメンテナンスの開始指示に引き続き、ＩＰｓｅｃセッションを確立することを目的とする。以下、図面により、本ＶＰＮセッション開始指示処理の詳細を説明する。

【０１０２】図７は、本発明の方法例に係るＶＰＮセッション開始指示処理を説明するためのフローチャートである（一部、リモートメンテナンス開始指示処理を含む）。

【０１０３】同図に示すように、本ＶＰＮセッション開始指示処理は、上述のリモートメンテナンス開始処理による起動を契機（Ｃ）に開始される。即ち、保守サーバ３のＶＰＮゲートウェイ設定処理部３３は、まず、端末１のルータ部１２をＩＰｓｅｃの対象ホストとした「ＩＰｓｅｃセッションの開始設定（ＶＰＮゲートウェイ４のｔｅｌｎｅｔコマンドの実装形態により異なる）」を

パラメータとしたｔｅｌｎｅｔコマンドを、ローカルネットワークセッションにより、ＶＰＮゲートウェイ４に向けて送信する（ＳＴ６２）。

【０１０４】ＶＰＮゲートウェイ４は、その設定コマンド受信処理部４２において、保守サーバ３から送信された上記コマンドを受信して（ＳＴ６３）、当該コマンドをＶＰＮ処理部４１へ受け渡し、さらに、このＶＰＮ処理部４１において、端末１のルータ部１２との間でＩＰｓｅｃを相互に確立する処理を実行して（ＳＴ６４，ＳＴ６５）、所要のＩＰｓｅｃのリンクを確立する（ＳＴ６６）。

【０１０５】次に、以上のＩＰｓｅｃの確立に伴い、ＶＰＮゲートウェイ４の設定コマンド受信処理部４２は、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとしたｔｅｌｎｅｔレスポンスを、ローカルネットワークセッションにより、保守サーバ３のＶＰＮゲートウェイ設定処理部３３に向けて送信する（ＳＴ６７）。

【０１０６】そして、保守サーバ３のＶＰＮゲートウェイ設定処理部３３は、ＶＰＮゲートウェイ４から送信された上記レスポンスを受信し（ＳＴ６８）、以上により、このＶＰＮセッション開始指示処理を完了して、処理を　のリモートメンテナンス開始指示処理へと引き戻す。

【０１０７】ここで、リモートメンテナンス開始指示処理は、上述のＶＰＮセッション開始指示処理における正常又は異常レスポンスの受信を契機（ＳＴ６８のステップ）に開始される。即ち、保守サーバ３のｈｔｔｐサーバ部３１は、上記レスポンスに対する「ステータス（ＩＰｓｅｃ確立又はエラーステータス）」をパラメータとしたｈｔｔｐレスポンスを、ローカルネットワークセッションにより、リモートメンテナンス装置６のメンテナンスコマンド処理部６１に向けて送信する（ＳＴ６９）。

【０１０８】そして、リモートメンテナンス装置６のメンテナンスコマンド処理部６１は、保守サーバ３から送信された上記レスポンスを受信し（ＳＴ７０）、以上により、このＶＰＮセッション開始指示処理を完了して、処理を　のリモートメンテナンス処理へと受け渡す。

【０１０９】なお、リモートメンテナンス装置６の後処理として、保守サーバ３から正常なＩＰｓｅｃ確立レスポンスが返送された場合には、後述する　のリモートメンテナンス処理を実行し、これに対し、エラーレスポンスが返送された場合には、端末１がインターネット２に接続されていないものと判断して、前述した　のリモートメンテナンス要求処理を再起動するよう、端末１の管理者に連絡することが必要である。

【０１１０】＜　リモートメンテナンス処理＞本リモートメンテナンス処理は、暗号化された伝送路としてのＩＰｓｅｃ等のＶＰＮトンネル７を経由して、リモートメンテナンス装置６からセキュアなリモートメンテナンスを実施し、端末１における故障を復旧することを目的とする。なお、ここで用いるリモートメンテナンス装置６は、特殊なものである必要はなく、ローカルネットワーク５上でコマンドを送信することにより、端末１をメンテナンスできる装置（例えば、ｈｔｔｐクライアント（ｗｅｂブラウザ）やｔｅｌｎｅｔツールなど）であれば、それを転用できる。また、その機能としては、ある故障（例えば、Ｐｒｏｘｙ故障）に関し、その復旧動作（Ｐｒｏｘｙの起動、端末１の再起動）を行う機能の他、例えば、端末１のログ表示や、ルータ部１２における各種設定の確認などを行う機能も具備する。以下、図面により、本リモートメンテナンス処理の詳細を説明する。

【０１１１】図８は、本発明の方法例に係るリモートメンテナンス処理を説明するためのフローチャートである。

【０１１２】同図に示すように、本リモートメンテナンス処理は、上述のリモートメンテナンス開始指示処理においてＩＰｓｅｃ確立レスポンスが返送されて以降、端末１がインターネット２に接続しており、ＶＰＮトンネル７が設定されている状態において、リモートメンテナンスの実施者の手動操作により任意の契機で開始される。即ち、リモートメンテナンス装置６のメンテナンスコマンド処理部６１は、「リモートメンテナンスコマンドであることを示すコード」，「リモートメンテナンスコマンド種別（サーバ部１１／ルータ部１２）」，及び「リモートメンテナンスコマンド詳細パラメータ」をパラメータとしたｈｔｔｐコマンドを、ＶＰＮセッションにより（ＶＰＮトンネル７を通じ）、端末１のサーバ部１１におけるｈｔｔｐサーバ部１１ａに向け送信する（ＳＴ７１）。

【０１１３】端末１のサーバ部１１では、リモートメンテナンス装置６から送信された上記コマンドを受信し（ＳＴ７２）、その受信に係るコマンド名及びパラメータを、まず、同端末１のＣＧＩ処理部１１ｂへ受け渡す。

【０１１４】ＣＧＩ処理部１１ｂは、上記コマンドがサーバ部１１へ対するものであった場合には、当該コマンド中のパラメータに応じて、所要のリモートメンテナンスの内部処理を実行し（ＳＴ７３）、これに対し、それがサーバ部１１ではなくルータ部１２へ対するものであった場合には、同端末１のルータ設定処理部１１ｃを介して、当該コマンドをルータ部１２へ転送して（ＳＴ７４）、そのコマンド中のパラメータに応じたリモートメンテナンスの内部処理を、当該ルータ部１２に実行させる（ＳＴ７５）。

【０１１５】そして、所要のリモートメンテナンスの内部処理が、端末１のサーバ部１１又はルータ部１２において実行されると、同端末１のｈｔｔｐサーバ部１１ａ

は、上記ＣＧＩ処理部１１ｂから、上記コマンドに対する「ステータス（正常又はエラーステータス）」を取得し、当該ステータスをパラメータとしたｈｔｔｐレスポンスを、ＶＰＮセッションにより（ＶＰＮトンネル７を通じ）、リモートメンテナンス装置６のメンテナンスコマンド処理部端末６１に向けて送信する（ＳＴ７６）。

【０１１６】そして、リモートメンテナンス装置６のメンテナンスコマンド処理部６１は、端末１から送信された上記レスポンスを受信し（ＳＴ７７）、以上により、このリモートメンテナンス処理を完了する。

【０１１７】＜　リモートメンテナンス終了指示処理＞
本リモートメンテナンス終了指示処理は、リモートメンテナンス装置６を使用して、実際にリモートメンテナンスを終了することを保守サーバ３に伝えることを目的とする。以下、図面により、本リモートメンテナンス終了指示処理の詳細を説明する。

【０１１８】図９は、本発明の方法例に係るリモートメンテナンス終了指示処理を説明するためのフローチャートである。

【０１１９】同図に示すように、本リモートメンテナンス終了指示処理は、リモートメンテナンスの実施者の手動操作により開始される。即ち、リモートメンテナンス装置６のメンテナンスコマンド処理部６１は、「リモートメンテナンス終了を示すコード」をパラメータとしたｈｔｔｐコマンドを、ローカルネットワークセッションにより、保守サーバ３のｈｔｔｐサーバ部３１に向け送信する（ＳＴ７８）。

【０１２０】
【外３】

保守サーバ３のｈｔｔｐサーバ部３１では、リモートメンテナンス装置６から送信された上記コマンドを受信し（ＳＴ７９）、以下、処理を⑩のＶＰＮセッション終了指示処理へと受け渡す（図示の記号「Ｅ」により連続）。

【０１２１】なお、本リモートメンテナンス終了指示処理は、実際には、以降に続くＶＰＮセッション終了指示処理が完了するまで起動状態を維持する。その詳細については、以下のＶＰＮセッション開始指示処理で併せて説明する（図示の記号「Ｆ」により連続）。

【０１２２】
【外４】

＜⑩ＶＰＮセッション終了指示処理＞
本ＶＰＮセッション終了指示処理は、上述のリモートメンテナンス終了指示処理の内部処理として機能し、リモートメンテナンスの終了指示に引き続き、ＩＰｓｅｃセッションを解除することを目的とする。以下、図面により、ＶＰＮセッション終了指示処理の詳細を説明する。

【０１２３】図１０は、本発明の方法例に係るＶＰＮセッション終了指示処理を説明するためのフローチャートである（一部、リモートメンテナンス終了指示処理を含む）。

【０１２４】同図に示すように、本ＶＰＮセッション終了指示処理は、上述のリモートメンテナンス終了処理による起動を契機（Ｅ）に開始される。即ち、保守サーバ３のＶＰＮゲートウェイ設定処理部３３は、まず、端末１のルータ部１２をＩＰｓｅｃの対象ホストとした「ＩＰｓｅｃセッションの終了設定（ＶＰＮゲートウェイ４のｔｅｌｎｅｔコマンドの実装形態により異なる）」をパラメータとしたｔｅｌｎｅｔコマンドを、ローカルネットワークセッションにより、ＶＰＮゲートウェイ４に向けて送信する（ＳＴ８０）。

【０１２５】ＶＰＮゲートウェイ４は、その設定コマンド受信処理部４２において、保守サーバ３から送信された上記コマンドを受信して（ＳＴ８１）、当該コマンドをＶＰＮ処理部４１へ受け渡し、さらに、このＶＰＮ処理部４１において、端末１のルータ部１２との間で確立されているＩＰｓｅｃを相互に終了する処理を実行すると共に（ＳＴ８２，ＳＴ８３）、ＩＰｓｅｃイニシエータ設定を消去して（ＳＴ８４）、ＩＰｓｅｃのリンクを終了する（ＳＴ８５）。

【０１２６】次に、以上のＩＰｓｅｃの終了に伴い、ＶＰＮゲートウェイ４の設定コマンド受信処理部４２は、上記コマンドに対する「ステータス（正常又はエラーステータス）」をパラメータとしたｔｅｌｎｅｔレスポンスを、ローカルネットワークセッションにより、保守サーバ３のＶＰＮゲートウェイ設定処理部３３に向けて送信する（ＳＴ８６）。

【０１２７】そして、保守サーバ３のＶＰＮゲートウェイ設定処理部３３は、ＶＰＮゲートウェイ４から送信された上記レスポンスを受信し（ＳＴ８７）、以上により、このＶＰＮセッション終了指示処理を完了して、処理を　のリモートメンテナンス終了指示処理へと引き戻す。

【０１２８】ここで、リモートメンテナンス終了指示処理は、上述のＶＰＮセッション終了指示処理における正常又は異常レスポンスの受信を契機（ＳＴ８７のステップ）に開始される。即ち、保守サーバ３のｈｔｔｐサーバ部３１は、上記レスポンスに対する「ステータス（ＩＰｓｅｃ確立又はエラーステータス）」をパラメータと

したｈｔｔｐレスポンスを、ローカルネットワークセッションにより、リモートメンテナンス装置６のメンテナンスコマンド処理部６１に向けて送信する（ＳＴ８８）。

【０１２９】そして、リモートメンテナンス装置６のメンテナンスコマンド処理部６１は、保守サーバ３から送信された上記レスポンスを受信し（ＳＴ８９）、以上により、このＶＰＮセッション終了指示処理を完了する。

【０１３０】なお、リモートメンテナンス装置６の後処理として、保守サーバ３から正常なＩＰｓｅｃ確立レスポンスが返送されたら、今回のリモートメンテナンス処理を終了する。

【０１３１】以上、本発明の実施の形態を、その適用システム構成例及び方法例につき説明したが、本発明は、必ずしも上述した手法にのみ限定されるものではなく、本発明にいう目的を達成し、後述の効果を有する範囲内において、適宜変更実施することが可能なものである。

【０１３２】例えば、以上に説明した方法例では、　のリモートメンテナンス開始指示処理が、リモートメンテナンスの実施者から手動操作により実行されて初めて、所要のＶＰＮトンネル７を確立させる場合を例に挙げたが、これに代え、　のＶＰＮゲートウェイ設定処理の終了後、　のリモートメンテナンス開始指示処理を実行することなしに、連続して　のＶＰＮセッション開始指示処理を起動、実行させることなども、無論可能である。この場合、端末１の故障通知後、連続的にＩＰｓｅｃが確立されることになる（何れの処理を採用するかについては、運用上のポリシーに委ねられる）。

【０１３３】

【外５】

また、同方法例では、最後に、⑨のリモートメンテナンス終了指示処理、及び⑩のＶＰＮセッション終了指示処理を実行する場合を例に挙げたが、これら各処理は、本発明にとって必須の要件ではなく、場合によっては、これらを省略するようにしてもよい。但し、無意味にＶＰＮセッションを継続させておくことは、端末１のセキュリティをいたずらに低下させることに等しいので、これら各処理の実行は、強く推奨されるものである。

【０１３４】

【発明の効果】以上、詳細に説明したように、本発明によれば、従来は人手が必要とされていた端末のメンテナンスを、インターネットを経由してリモートで実施することが可能となることから、保守稼働の低減、並びに、通信費用や派遣費用などの保守コストの軽減を図ることができる。

【０１３５】また、従来は、セキュリティレベルの確保のために、リモートメンテナンス用の独自の暗号処理技術等が必要であったが、本発明によれば、下位のＩＰｓｅｃレベルにおいて暗号処理及び認証処理を行うことにより、十分なセキュリティが確保されるため、例えば、ルータメンテナンスのアプリケーションを、端末の内線からの制御と、リモートメンテナンス制御とに共通して利用することなども可能となる。この結果、アプリケーションの開発コスト及び維持コストを、大いに削減することができる。

【図面の簡単な説明】

【図１】本発明の適用システムであるリモートメンテナンスシステムの構成を示す図である。

【図２】本発明の方法例に係る設置通知処理を説明するためのフローチャートである。

【図３】本発明の方法例に係る端末ＶＰＮ鍵設定処理を説明するためのフローチャートである。

【図４】本発明の方法例に係る故障通知処理を説明するためのフローチャートである。

【図５】本発明の方法例に係るリモートメンテナンス要求処理及びＶＰＮゲートウェイ設定処理を説明するためのフローチャートである。

【図６】本発明の方法例に係るリモートメンテナンス開始指示処理を説明するためのフローチャートである。

【図７】本発明の方法例に係るＶＰＮセッション開始指示処理を説明するためのフローチャートである。

【図８】本発明の方法例に係るリモートメンテナンス処理を説明するためのフローチャートである。

【図９】本発明の方法例に係るリモートメンテナンス終了指示処理を説明するためのフローチャートである。

【図１０】本発明の方法例に係るＶＰＮセッション終了指示処理を説明するためのフローチャートである。

【符号の説明】

α…リモートメンテナンスシステム（適用システム）
１…端末
１１…サーバ部
１１ａ…ｈｔｔｐサーバ部
１１ｂ…ＣＧＩ処理部
１１ｃ…ルータ設定処理部
１１ｄ…故障検出処理部
１１ｅ…コマンド送信処理部
１２…ルータ部
２…インターネット
３…保守サーバ
３１…ｈｔｔｐサーバ部
３２…ＣＧＩ処理部
３３…ＶＰＮゲートウェイ設定処理部
４…ＶＰＮゲートウェイ
４１…ＶＰＮ処理部

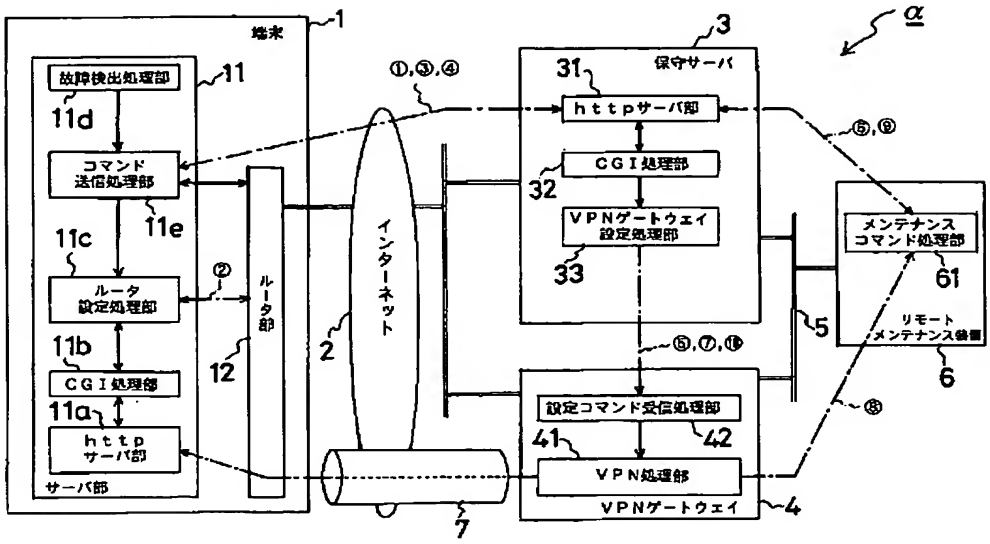
27

４２…設定コマンド受信処理部
５…ローカルネットワーク
６…リモートメンテナンス装置

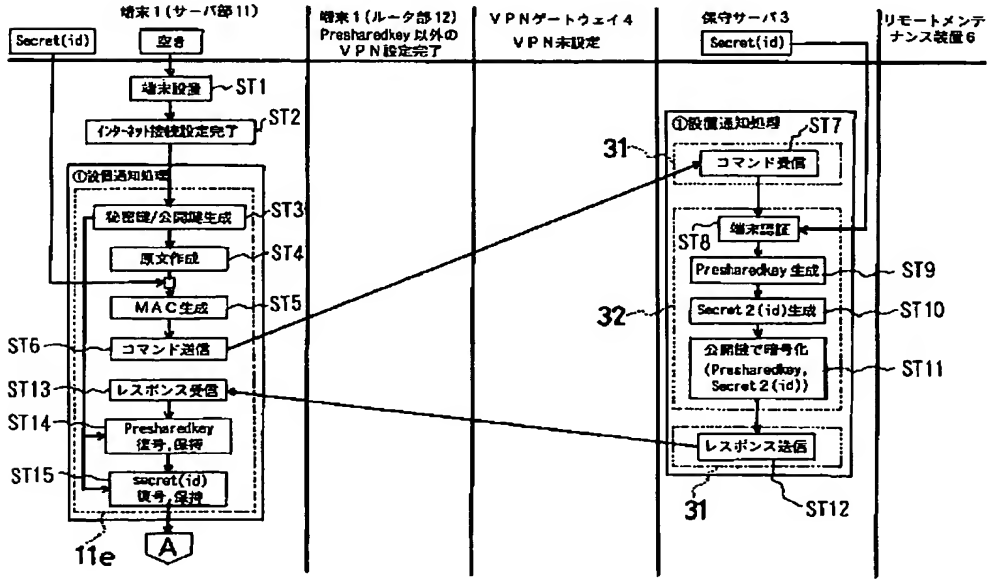
28

６１…メンテナンスコマンド処理部
７…ＶＰＮトンネル

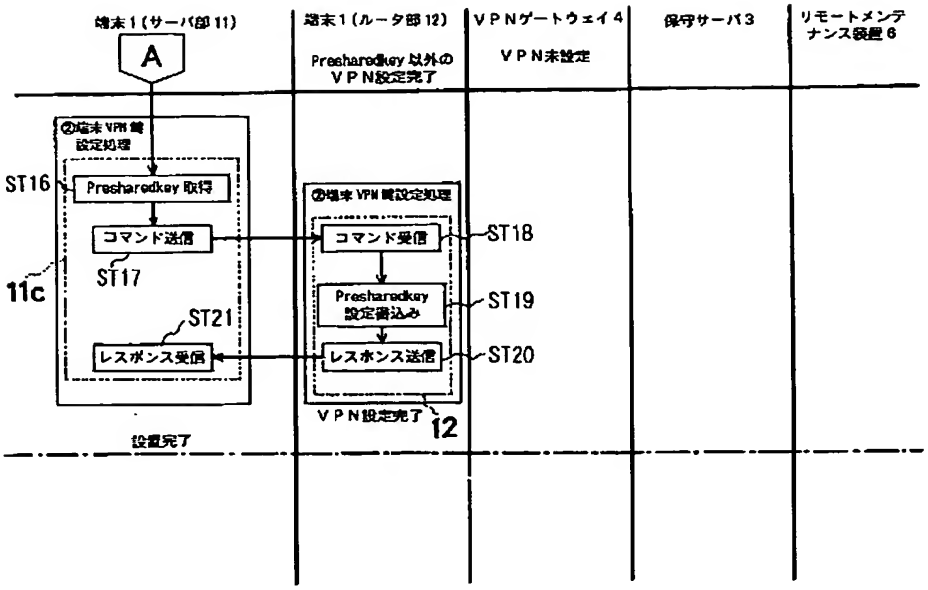
【図１】



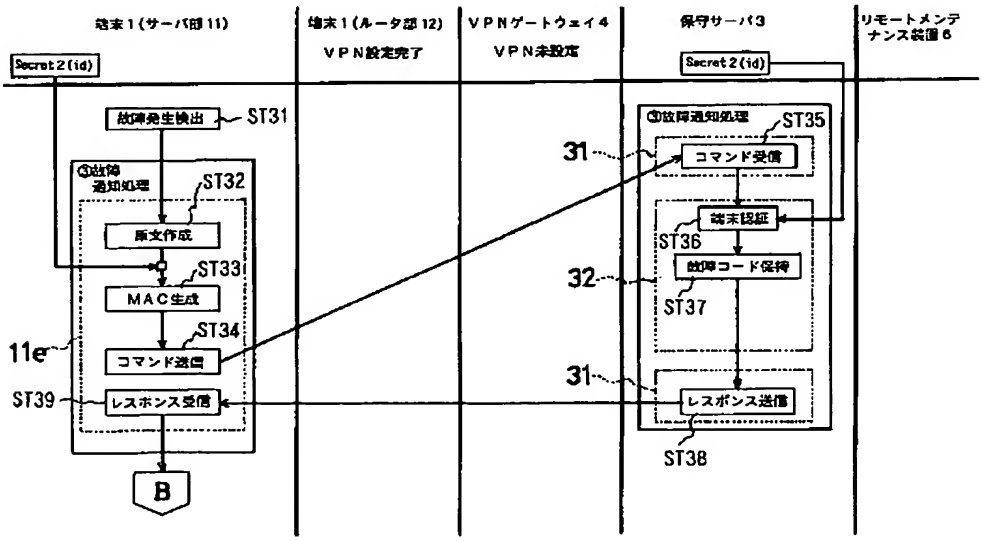
【図２】



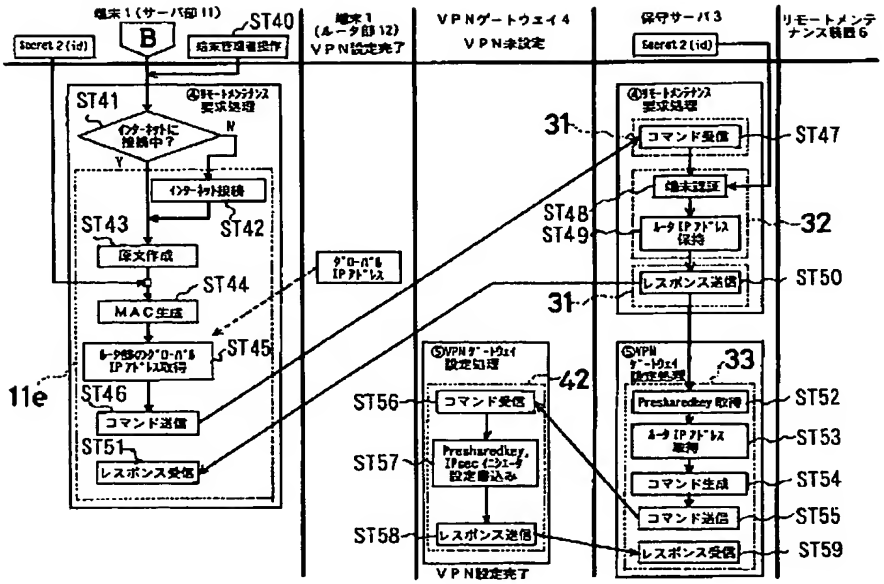
【図３】


端末１(サーバ部11)
端末１(ルータ部12)
VPNゲートウェイ４
保守サーバ３
リモートメンテナンス装置６
A
Presharedkey 以外のVPN設定完了
VPN未設定
②端末VPN鍵設定処理
ST16
Presharedkey 取得
コマンド送信
ST17
11c
ST21
レスポンス受信
③端末VPN鍵設定処理
コマンド受信
ST18
Presharedkey設定書込み
ST19
レスポンス送信
ST20
VPN設定完了
12
設置完了

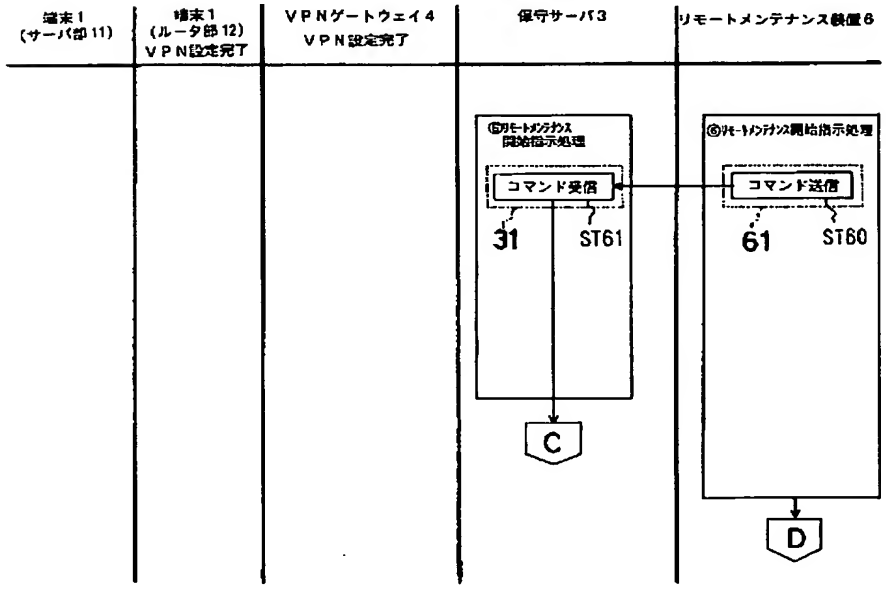
【図４】


端末１(サーバ部11)
端末１(ルータ部12)
VPNゲートウェイ４
保守サーバ３
リモートメンテナンス装置６
Secret2(id)
VPN設定完了
VPN未設定
Secret2(id)
故障発生検出
ST31
③故障通知処理
ST32
原文作成
ST33
MAC生成
ST34
11e
コマンド送信
ST39
レスポンス受信
B
31
③故障通知処理
ST35
コマンド受信
端末認証
ST36
故障コード保持
32
ST37
31
レスポンス送信
ST38

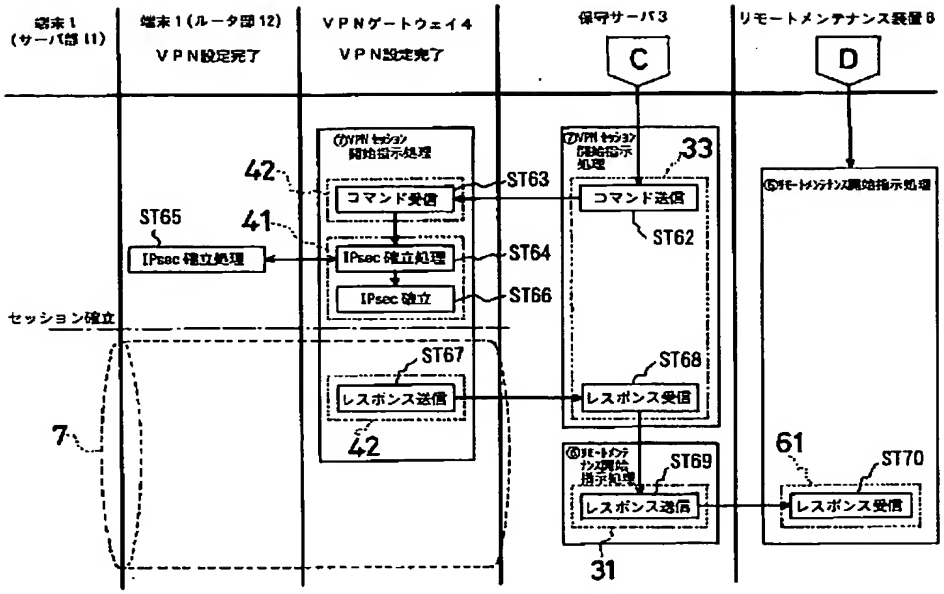
【図５】


端末１（サーバ部１１）
B
ST40
端末管理者操作
端末１（ルータ部１２）VPN設定完了
VPNゲートウェイ４ VPN未設定
保守サーバ３
リモートメンテナンス装置６
Secret２(id)
ST41
インターネットに接続中？
N
Y
インターネット接続
ST42
ST43
署名作成
ST44
MAC生成
ST45
ST46
コマンド送信
ST51
レスポンス受信
11e
グローバルIPアドレス
31
コマンド受信
ST47
端末認証
ST48
ST49
ルータIPアドレス保持
32
レスポンス送信
ST50
31
33
Presharedkey取得
ST52
ルータIPアドレス取得
ST53
コマンド生成
ST54
コマンド送信
ST55
レスポンス受信
ST59
42
ST56
コマンド受信
ST57
Presharedkey, IPsecパラメータ設定書込み
ST58
レスポンス送信
VPN設定完了

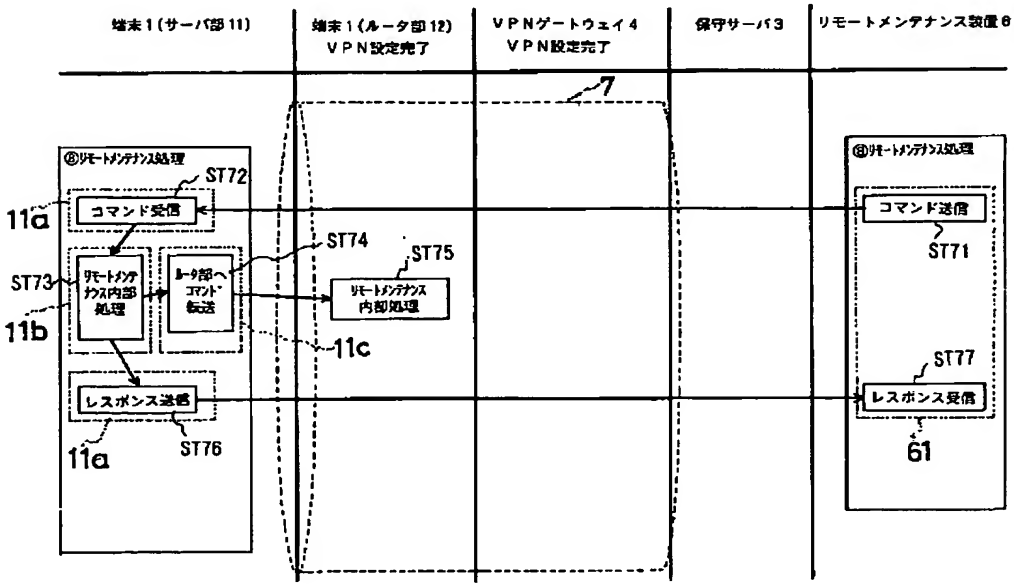
【図６】


端末１（サーバ部１１）
端末１（ルータ部１２）VPN設定完了
VPNゲートウェイ４ VPN設定完了
保守サーバ３
リモートメンテナンス装置６
コマンド受信
31
ST61
C
コマンド送信
61
ST60
D

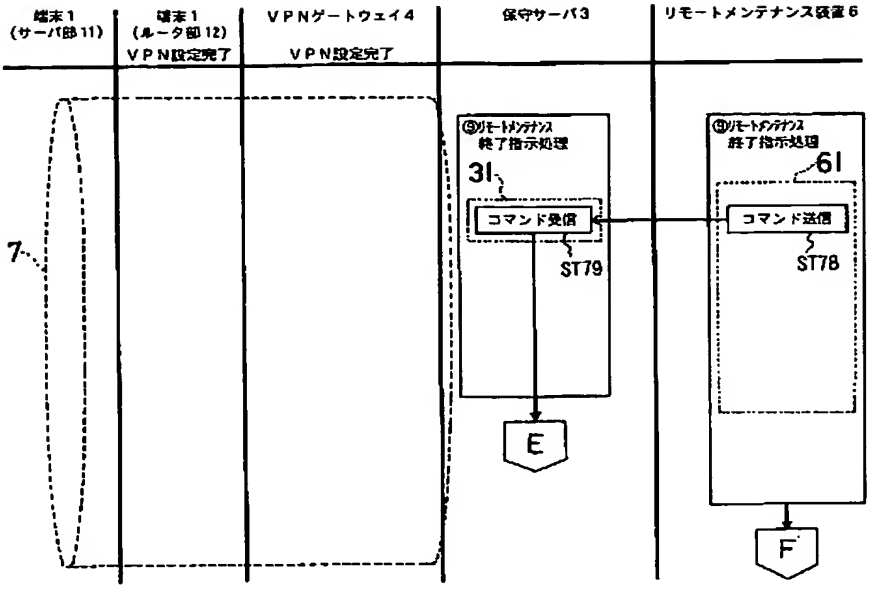
【図７】


端末１
（サーバ部１１）
端末１（ルータ部１２）
ＶＰＮ設定完了
ＶＰＮゲートウェイ４
ＶＰＮ設定完了
保守サーバ３
リモートメンテナンス装置８
C
D
42
41
33
ST63
ST65
ST64
ST66
ST62
コマンド受信
コマンド送信
IPsec 確立処理
IPsec 確立
セッション確立
ST67
ST68
ST69
ST70
レスポンス送信
レスポンス受信
7
61
31

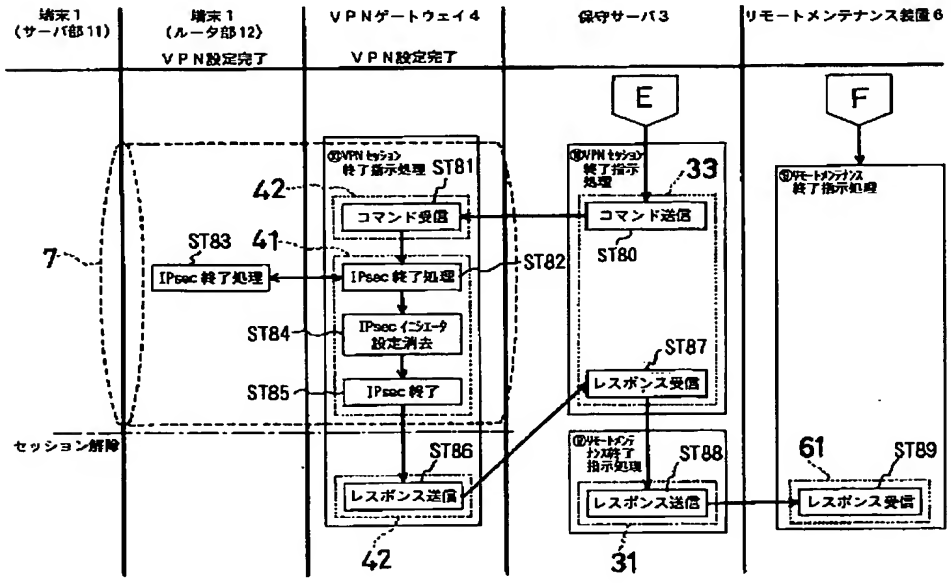
【図８】


端末１（サーバ部１１）
端末１（ルータ部１２）
ＶＰＮ設定完了
ＶＰＮゲートウェイ４
ＶＰＮ設定完了
保守サーバ３
リモートメンテナンス装置８
7
ST72
ST71
ST74
ST75
ST73
ST77
ST76
11a
11b
11c
コマンド受信
コマンド送信
レスポンス送信
レスポンス受信
61

【図９】


端末１
（サーバ部１１）
端末１
（ルータ部１２）
ＶＰＮ設定完了
ＶＰＮゲートウェイ４
ＶＰＮ設定完了
保守サーバ３
リモートメンテナンス装置６
⑤リモートメンテナンス
終了指示処理
31
コマンド受信
ST79
⑤リモートメンテナンス
終了指示処理
61
コマンド送信
ST78
7
E
F

【図１０】


端末１
（サーバ部１１）
端末１
（ルータ部１２）
ＶＰＮ設定完了
ＶＰＮゲートウェイ４
ＶＰＮ設定完了
保守サーバ３
リモートメンテナンス装置６
E
F
⑥VPN セッション
終了指示処理
ST81
42
コマンド受信
ST83
41
IPsec 終了処理
ST82
ST84
IPsec イニシエータ
設定消去
ST85
IPsec 終了
ST86
レスポンス送信
42
⑥VPN セッション
終了指示処理
33
コマンド送信
ST80
ST87
レスポンス受信
⑫リモートメンテナンス
終了指示処理
ST88
レスポンス送信
31
⑤リモートメンテナンス
終了指示処理
61
ST89
レスポンス受信
7
セッション解除